MISSOURI CIRCUIT COURT
TWENTY-SECOND JUDICIAL CIRCUIT
CITY OF ST. LOUIS

JOHN DOE I and JOHN DOE II, on behalf of themselves and all others similarly situated, *Plaintiffs*, v. BJC HEALTH SYSTEM d/b/a BJC HEALTHCARE, Serve: CSC-Lawyers Incorporating Service Co. 221 Bolivar St. Jefferson City, MO 65101 *Defendant*.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION PETITION

COME NOW Plaintiffs John Doe I and John Doe II, by and through counsel and on behalf of themselves and all others similarly situated, upon personal knowledge as to Plaintiffs' own conduct and on information and belief as to all other matters based upon investigation of counsel, such that each allegation has evidentiary support or is likely to have evidentiary support upon further investigation and discovery, and for their Class action Petition against Defendant BJC Health System ("BJC" or "BJC Healthcare"), states as follows:

PARTIES TO THE ACTION

1. Plaintiff John Doe I is a resident of St. Louis County, Missouri; BJC patient; and MyChart patient portal user.

2. Plaintiff John Doe II is a resident of St. Charles County, Missouri; BJC patient; and MyChart patient portal user.

3. Defendant BJC Health System is a Missouri non-profit corporation headquartered at 901 Forest Park Avenue, Suite 1200, St. Louis, MO 63108.

JURISDICTION AND VENUE

4. At all times relevant herein, BJC Health System is and was a Missouri nonprofit corporation in good standing, doing business in the State of Missouri. BJC may sue or be sued in its own name with offices, agents and its principal place of business within St. Louis City, State of Missouri.

5. At all times relevant herein, BJC was in the business of providing health care to members of the public.

6. Venue is proper in the Circuit Court of St. Louis City pursuant to Mo. Rev. Stat. §§ 508.010.4 and 508.010.8 because Plaintiffs were first injured in St. Louis City, State of Missouri.

7. Venue is also proper in the Circuit Court of St. Louis City pursuant to Mo. Rev. Stat. § 407.025 because the acts complained of occurred in St. Louis City and Defendant is headquartered in St. Louis City.

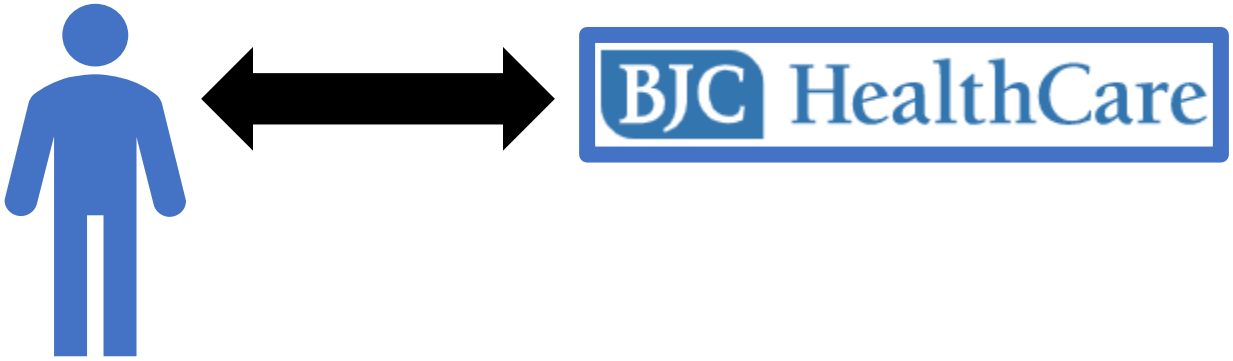
NATURE OF THE ACTION

8. Medical providers have a duty to patients to keep patient data, communications, diagnoses, and treatment information completely confidential unless authorized to make disclosures by the patient.

9. Patients are aware of the promises of confidentiality contained within the Hippocratic Oath and protected by statutory, regulatory, and common law and must be able to rely on those promises, obligations, and expectations.

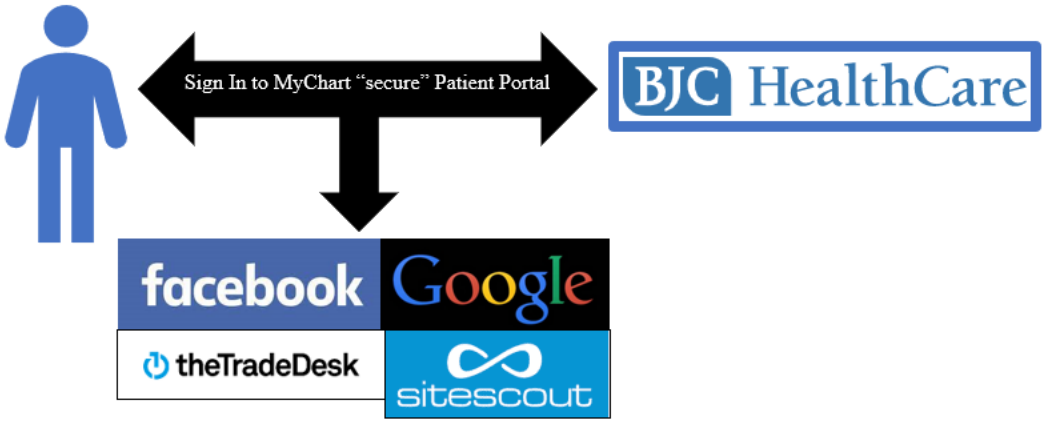
10. A patient who exchanges communications with Defendant has a reasonable expectation of privacy that their personally identifiable data and the content of their communications will not be transmitted or re-directed by Defendant to third parties without the patient's knowledge, consent, authorization, or any further action on their part.

11. Based on patients' reasonable expectations of privacy and Defendant's public promises, a patient would believe the following illustrates their communications exchanged with BJC:



12. Despite its ethical and legal obligations and its patients' reasonable expectations of privacy, Defendant systematically violated the medical privacy rights of its patients by causing the contemporaneous unauthorized transmission of personally identifiable patient data and re-direction of the precise content of patient communications with BJC to be sent to Facebook, Google, SiteScout, Invoca, and theTradeDesk without patient knowledge, consent, authorization, or any affirmative action.

13. BJC's true data practices are illustrated as follows:



14. Defendant's conduct gives rise to at least five causes of action: (1) breach of fiduciary duty of confidentiality; (2) intrusion upon seclusion; (3) violations of Missouri computer crime laws in §§ 569.095 to 569.099, RSMo; (4) identity theft in violation of § 570.223, RSMo; and (5) violation of the Missouri Merchandising Practices Act, § 407.010, RSMo *et seq*.

15. As a result of Defendant's conduct in disclosing personally identifiable patient data and the content of patient communications to third parties without patient knowledge, consent, authorization, or any further action by the patient, Defendant has caused damaged to Plaintiffs and other patient Class Members in that:

a. Sensitive and confidential information that Plaintiffs and patient Class members intended to remain private is no more;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. Defendant took something of value from Plaintiffs and patient Class members and derived benefit therefrom without Plaintiffs and Class members' knowledge or informed consent or authorization and without sharing the benefit of such value;

d. Plaintiffs and other patient Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiffs and Class members' personal information.

FACTS APPLICABLE TO ALL COUNTS

Patients Have Reasonable Expectations of Privacy

16. Plaintiffs are patients of BJC and a users of the MyChart patient portal.

17. As a patient, Plaintiffs have a reasonable expectation of privacy that BJC, their health care provider, and its business associates, including Epic Software Systems, will not disclose their personally identifiable information and the content of their communications to third parties without their express authorization.

18. Plaintiffs' and other patients' reasonable expectations privacy in their personally identifiable data and communications exchanged with BJC are grounded in:

a. BJC's status as Plaintiffs' health care provider;

b. BJC's common law obligation to maintain the confidentiality of patient data and communications;

c. State and federal laws and regulations protecting the confidentiality of medical information;

d. State and federal laws protecting the confidentiality of communications and computer data;

e. State laws protecting unauthorized use of personal means of identification;

f. Defendants' express promises of confidentiality; and

g. Defendants' implied promises of confidentiality.

The BJC Web-Property

19. BJC maintains various web-properties, including www.bjc.org and www.barnesjewish.org, for its patients to communicate with BJC, including but not limited to exchanging communications about bill payment, doctors, services, treatments, conditions, appointments, and access to an online MyChart patient portal.

20. BJC actively encourages patients to use the www.bjc.org web property.

21. Plaintiffs exchanged communications with BJC at its web property.

22. BJC's homepage shows how the web property is designed for use by patients. The homepage provides patients with tools to "Find a Provider," "Find a Location," schedule "Virtual Care," "Schedule Your Vaccine," "Access MyChart," and "Skip the Waiting Room."

The MyChart Patient Portal

23. BJC also maintains a patient portal, www.bjc.org/MyChart, for its patients to communicate with BJC, including but not limited to "request medical appointments," "view your health summary," "view test results," "request prescription renewals," "access trusted health information resources," and "communicate electronically and securely with your medical care team."

24. The BJC patient portal is "owned and operated by MyChart," a software system designed and licensed to BJC by Epic Software Systems ("Epic").

25. Epic is a privately owned health care software company that provides services to 250 million patients, including two thirds of the US population.

26. Epic is a "developer-led" company that builds its software systems "in-house."[1]

27. Epic states its software "offers patients personalized and secure online access to portions of their medical records" and "enables you to securely use the Internet to help manage and receive information about your health. With MyChart, you can:

- Request medical appointments.
- View your health summary.
- View test results.
- Request prescription renewals.
- Access trusted health information resources.
- Communicate electronically and securely with your medical care team."[2]

28. BJC publicly represents that "We take great care to ensure your health information is kept private and secure" and that "MyChart. . .is fully compliant with federal and state laws

[1] *About Us,* Epic, https://www.epic.com/about (last visited July 15, 2022).
[2] *MyChart*, BJC HealthCare, https://www.bjc.org/MyChart (last visited July 15, 2022).

pertaining to your privacy. Your name and email address will be treated with the same care and privacy given your health records and will never be sold or leased by MyChart."[3]

29. Despite these promises, Epic's MyChart software system was designed to permit licensees—such as BJC—to deploy "custom analytics scripts" within MyChart including, for example, Google Analytics. Feathers, T., *Pixel Hunt: Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022) (available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites).

30. Defendants took advantage of MyChart's analytics compatibility by knowingly and secretly deploying Google source code *inside the patient portal* that causes the contemporaneous unauthorized transmission of personally identifiable patient data and re-direction of the precise content of patient communications with BJC to be sent to Google.

31. Like its other web properties, BJC actively encourages patients to use the MyChart patient portal.

32. As a BJC patient and MyChart patient portal user, Plaintiffs exchanged communications with BJC through its web properties, including the MyChart portal.

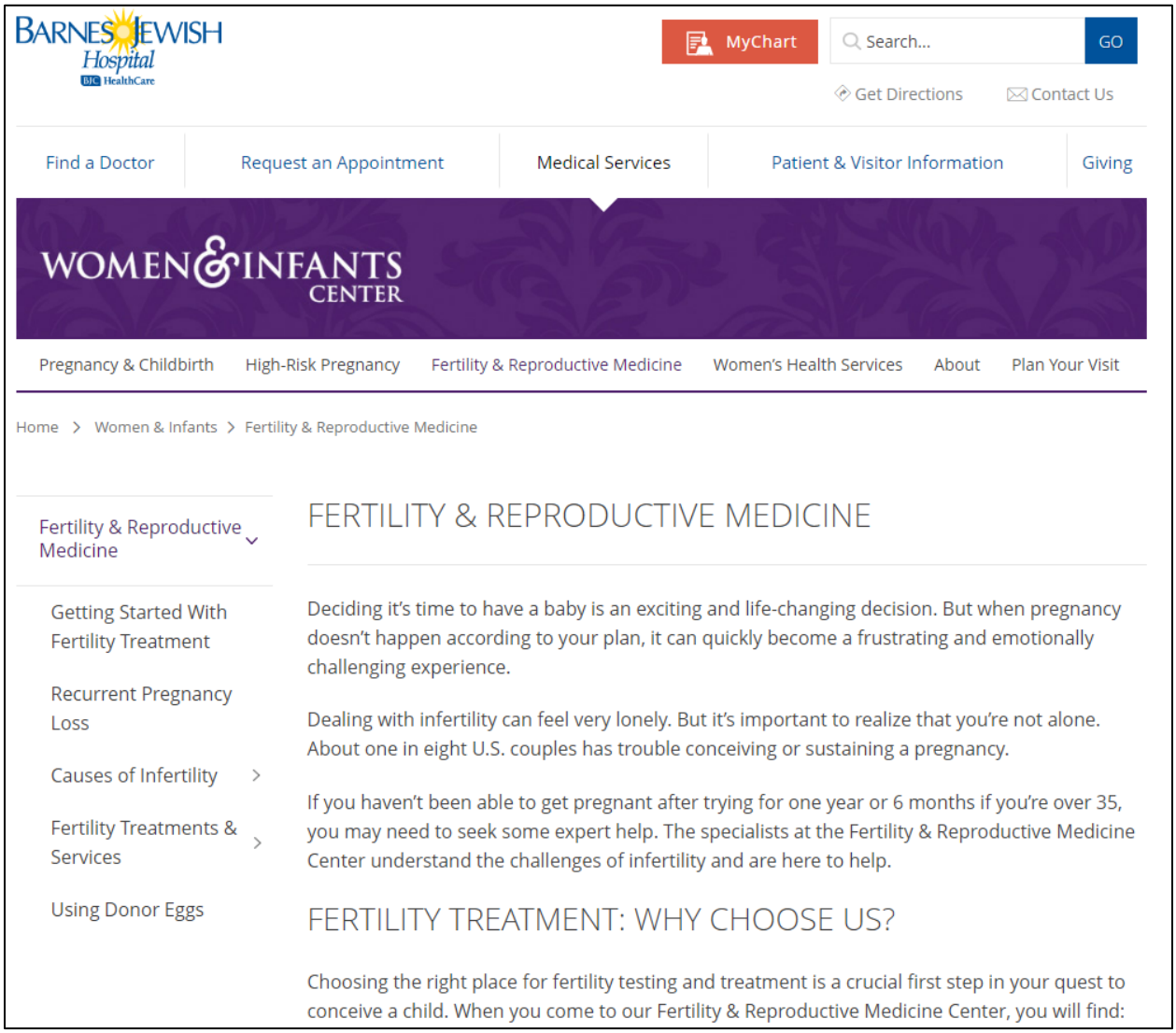
BJC Secretly Transmits Personally Identifiable Patient Data and Re-directs the Content of Patient Communications to Third Parties

33. Web browsers are software applications that allow consumer to exchange electronic communications over the Internet.

[3] *MyChart Frequently Asked Questions*, BJC HealthCare, https://www.mypatientchart.org/mychart/Authentication/Login?mode=stdfile&option=faq (last visit July 15, 2022).

34. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

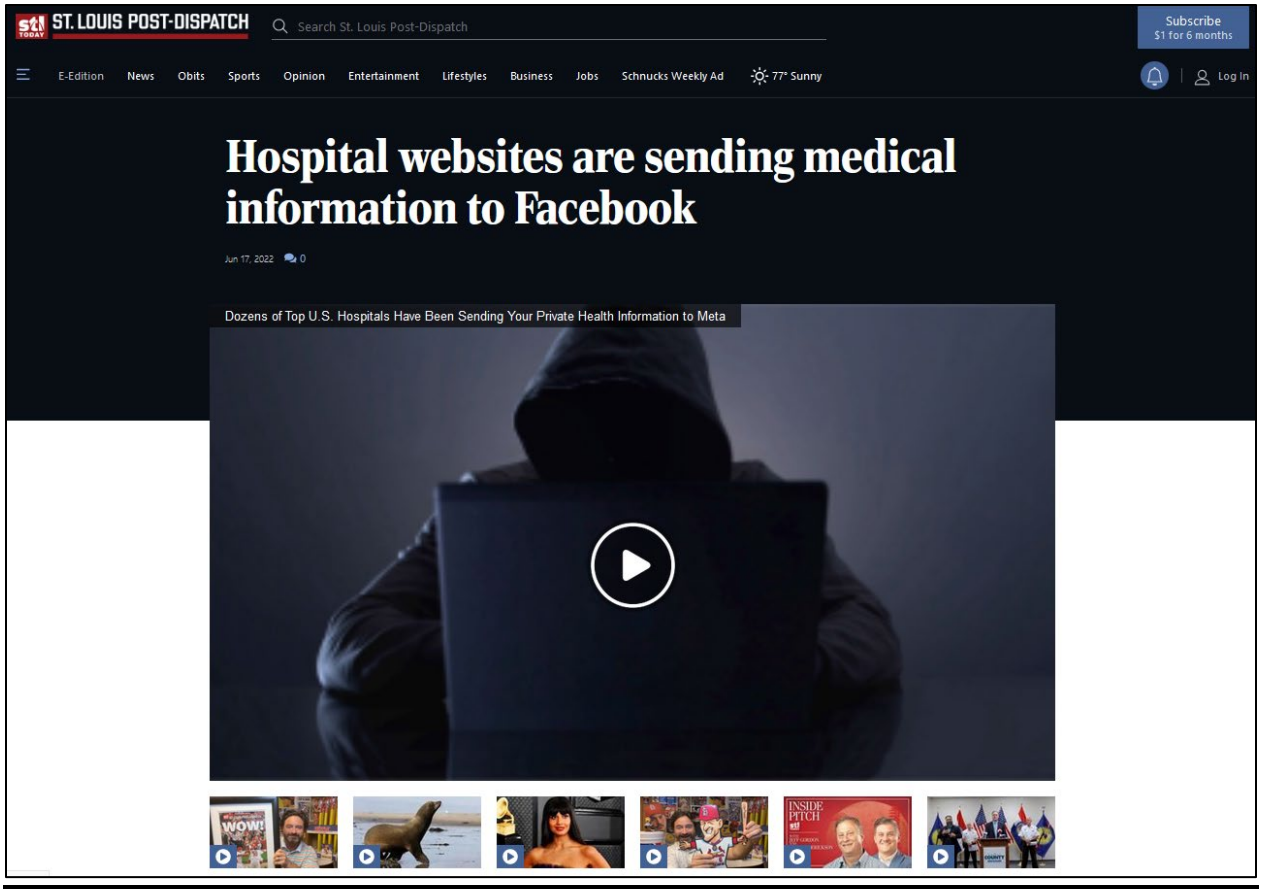
35. The basic command web browsers use to communicate with website servers is called a GET request. When a patient types https://www.barnesjewish.org/Medical-Services/Women-Infants/Fertility-Reproductive-Medicine into the navigation bar of his or her web-browser (or, just as, if not more frequently, takes the technological shortcut of clicking a hyperlink), the patient's web-browser makes connection with the server for BJC and sends the following: "GET /Medical-Services/Women-Infants/Fertility-Reproductive-Medicine HTTP/1.1"



36. The other basic request utilized by web browsers is a POST request, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or a submit button. 'POST' sends the data entered in the form to the server for the website.

37. In response to receiving a GET or POST request, the server for the entity with which the user is exchanging communications will send a set of instructions to the web-browser, commanding the browser with source code that (1) directs the browser on how to render the entity's response and, in many circumstances, (2) commands the browser to transmit personally identifiable data about the Internet user and re-direct the precise content of the user's GET or POST requests to various third parties.

38. In some circumstances, the third parties to whom user's communications are re-directed help the entity display actual substantive content on the webpage relating to the user's communications exchange with the website. For example, an article, "Hospital websites are sending medical information to Facebook" published on the St. Louis Post Dispatch website www.stltoday.com on July 17, 2022, features the following video link which is hosted by a third party:



39. In other cases, the third parties to whom user data is transmitted and the content of communications redirected provide no substantive content relating to the communications exchanged between the user and the website. These third parties are typically procured by websites to track users' personally identifiable data and communications for marketing purposes.

40. In many such cases, the third parties acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screened) called a web bug, tracking pixel, or web beacons. These web-bugs are tiny and camouflaged to purposefully remain invisible to the user.

41. Web bugs can be placed directly on a page by a web developer or can be funneled through a "tag manager" service to make the invisible tracking run more efficiently and to further obscure the third parties to whom the website transmits personally identifiable user data and re-directs the content of communications.

42. In the absence of a tag manager, a website developer who chooses to deploy third party source code on their website must enter the third-party source code directly onto their website for every third-party to whom they seek to transmit and re-direct user data and communications. On websites with several third-party trackers, this may cause the page to load more slowly and increases risk of a coding error, effecting functionality and usability. A "tag manager" offers the website developer a vessel in which to place all third-party source code. Instead of placing all third-party source code directly on the webpage, the developer places the source code within its account at the tag manager.

43. Google explains the benefits of Google Tag Manager in an Introduction to Google Tag Manager video on YouTube. [4] Google explains:

> Tags on your website help you measure traffic and optimize your online marketing. But all that code is cumbersome to manage. It often takes too long to get new tags on your site or update existing ones. This can delay campaigns by weeks or months so you miss valuable opportunities, data, and sales. That's where tag management comes in. Google Tag Manager is a powerful free tool that puts you the marketer back in control of your digital marketing. You update all your tags from Google Tag Manager instead of editing the site code. This reduces errors, frees you from having to involve a web master, and lets you quickly deploy tags on your site.
>
> Here's how it works. Sign in with an existing Google Account. Go to Google.com/tagmanager and create an account for your company. We'll name this one after the name of our company, Example Inc. Next, create a container for your domain name. We'll name this one after our website, example.com. This container will hold all the tags on the site. When you create a container, Google Tag Manager generates a container snippet to add to your site. Copy this container snippet and paste it into every page of your site. Paste the snippet below the opening body tag. Once you've pasted the container snippet into your site, you add and edit your tags using Google Tag Manager. You can add any marketing or measurement tag you want, whenever you want.

44. BJC deploys Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the BJC web property that is, in reality, an invisible window through

[4] See https://www.youtube.com/watch?v=KRvbFpeZ11Y, audio from 0:04 to 1:40.

which BJC funnels web bugs for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

45. BJC's Google Tag Manager source code is designed to be invisible. On "brain tumors" communications page set forth above, the GTM source code used by BJC specifies an "iframe" with a height of 0, width of 0, display of none, and visibility of hidden.

```
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-5T8CBJ');</script>
<!-- End Google Tag Manager -->
<!-- Google Tag Manager -->
<script>
    (function(w,d,s,l,i){w[l]=w[l]||[];
    w[l].push({'gtm.start':new Date().getTime(),event:'gtm.js'});
    var f=d.getElementsByTagName(s)[0],j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';
    j.async=true;
    j.src='https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
    })(window,document,'script','dataLayer','GTM-KGSK9J3');
</script>
<!-- End Google Tag Manager -->
```

****

```
<!-- Google Tag Manager (noscript) -->
<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-5T8CBJ"
height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
<!-- End Google Tag Manager (noscript) -->
<!-- Google Tag Manager (noscript) -->
<noscript>
    <iframe src="https://www.googletagmanager.com/ns.html?id=GTM-KGSK9J3"height="0" width="0" style="display:none;
    visibility:hidden">
    </iframe>

</noscript>
<!-- End Google Tag Manager (noscript) -->
```

46. BJC then funnels invisible 1x1 web bugs or pixels through this purposefully invisible iframe to help third-parties track, acquire, and record patient data and communications.

47. By design, none of the tracking is visible to patients at the BJC web property.

48. For example, the reproductive medicine page above does not include anything to apprise patients that BJC is causing their personally identifiable data to be transmitted and the content of their communications re-directed to Facebook, Google, SiteScout, Invoca, and theTradeDesk.

The Forms of Patient Personally Identifiable Information that Defendants

Causes to Be Transmitted to Third-Party Marketing Companies

49. BJC's MyChart portal co-owner Washington University Physicians ("WUP") maintains a list of identifiers that are considered personally identifiable health information for compliance purposes. This list includes:

HIPAA Identifiers

What are the HIPAA identifiers?

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
   - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
   - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Photographs/Videos.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

HIPAA Identifiers, Washington University in St. Louis, https://hipaa.wustl.edu/resources/hipaa-identifiers/ (last visited July 15, 2022).

50. WUP's internal policies further define electronic protected health information ("ePHI") as "Protected Health Information that this produced, saved, transferred, or received in

an electronic form (such as email or text)."[5] This includes "the combination of health information with one or more of the designated HIPAA identifiers."

51. Furthermore, this ePHI policy explicitly states that it includes "Barnes Jewish Hospital." *Id.*

52. Despite its own legal obligations and internal policies, Defendant's source code causes transmission of the following PHI to third parties:

a. Patient IP addresses;

b. Unique, persistent patient cookie identifiers;

c. Device identifiers;

d. Account numbers;

e. URLs;

f. Other unique identifying numbers, characteristics, or codes; and

g. Browser-fingerprints.

53. Defendant causes transmission and uses these patient identifiers without patient knowledge, consent, authorization, or any further action by the patient.

IP Addresses are Personally Identifiable

54. An IP address is a number that identifies a computer connected to the Internet.

55. IP addresses are used to identify and route communications on the Internet.

56. IP addresses of individual Internet users are used by websites and tracking companies to facilitate and track Internet communications.

[5] *ePHI*, Washington University in St. Louis, https://hipaa.wustl.edu/resources/ephi/ (last visited July 15, 2022).

57. Individual homes and their occupants can be, and are, tracked and targeted with advertising using IP addresses.

58. Under the Health Insurance Portability and Accountability Act ("HIPAA"), an IP address is considered personally identifiable information. See 45 C.F.R. § 164.514(b)(2)(i)(O).

59. Defendant uses and causes the disclosure of patient IP addresses to third parties with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the Patient Portal.

Internet Cookies are Personally Identifiable

60. In the early years of the Internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

61. Computer programmers eventually developed "cookies" – small text files that web servers can place on a person's web browser and computing device when that person's web browser interacts with the website server. Cookies can perform different functions. Eventually, some cookies were designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

62. Cookies are designed to and, in fact, do operate as means of identification for Internet users.

63. Cookies are protected personal identifiers under HIPAA. See 45 C.F.R. § 164.514(b)(2)(i)(H), (J), (M), (N), and (R).

64. In general, cookies are categorized by (1) duration and (2) party.

65. There are two types of cookies classified by duration:

a. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.

b. "Persistent cookies" are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's Internet communications for years and over dozens or hundreds of websites. Persistent cookies are sometimes called "tracking cookies."

66. Cookies are also classified by the party that uses the collected data.

a. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. For example, Defendant set a collection of its own cookies on patients' browsers when they visit any webpage on Defendant's web properties. First-party cookies can be helpful to the user, server, and/or website to assist with security, log in, and functionality.

b. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits www.bjc.org will also have cookies on their device from third parties, such as Facebook. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

67. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to that person's communications and habits. To build individual profiles of Internet users, third party data companies assign each user a unique, or a set of unique identifiers to each user.

68. Traditionally, first- and third-party cookies were kept separate. An Internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although BJC can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record the patient's communications, it is not permitted direct access to Facebook third-party cookie values. The reverse was also true: Facebook was not provided direct access to the values associated with first-party cookies set by BJC.

69. Data companies have designed a way to hack around the same-origin policy so that third-party data companies gain access to first-party cookies.

70. Javascript source code developed by third-party data companies and placed on a webpage by a developer such as BJC can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information they have collected and recorded about a user that is associated with a cookie identification number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

71. Defendant uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the Patient Portal.

72. Defendant's cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that Defendant assigns to patients to be made to third parties.

Browser-Fingerprints are Personally Identifiable

73. A browser-fingerprint is information collected about a computing device that can be used to identify the device.

74. A browser-fingerprint can be used to identify a device when the device's IP address is hidden and cookies are blocked.

75. The Electronic Frontier Foundation has explained:

> When a site you visit uses browser fingerprinting, it can learn enough information about your browser to uniquely distinguish you from all the other visitors to that site. Browser fingerprinting can be used to track users just as cookies do, but using much more subtle and hard-to-control techniques. In a paper EFF released in 2010, we found that a majority of users' browsers were uniquely identifiable given existing fingerprinting techniques. Those techniques have only gotten more complex and obscure in the intervening years. By using browser fingerprinting to piece together information about your browser and your actions online, trackers can covertly identify users over time, track them across websites, and building an advertising profile of them.[6]

[6] Katarzyna Szymielewicz and Bill Dudington, *The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers*, Electronic Frontier Foundation (June 19, 2018) (available at https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers).

76. In 2017, researchers showed that browser fingerprinting techniques can successfully identify 99.24 percent of users.[7]

77. Browser-fingerprints are protected personal identifiers under HIPAA. See 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

78. BJC uses and causes the disclosure of data sufficient to form a browser-fingerprint with each re-directed communication described herein, including patient communications about providers, conditions, treatments, appointments, bills, registration, and log-ins to the Patient Portal.

THE THIRD PARTIES TO WHOM BJC CAUSES DISCLOSURES OF PATIENT COMMUNICATIONS AND PII

Google

79. By many measures, Google is the world's largest data company. Among other services, Google operates the world's most popular search engine (Google), email provider (Gmail), video website (YouTube), mapping service (Google Maps), Internet analytics service for web developers (Google Analytics), and web-browser (Chrome). It also operates various ad services that are among the world's most popular in their respective category, including the advertising services of Google DoubleClick and Google AdWords.

80. Google Analytics has massive reach. As described by the Wall Street Journal, it is "far and away the web's most dominant analytics platform" and "tracks you whether or not you are logged in."[8]

---

[7] Yinzhi Cao, Song Li and Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, Proceedings of the Network and Distributed Security Symposium (March 2017) (available at http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf).

[8] *Who Has More of Your Personal Data than Facebook? Try Google*, The Wall Street Journal (April 22, 2018) (available at https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401).

81. Google tracks Internet users with IP addresses, cookies, geolocation, and other unique device identifiers.

82. Google cookies are personally identifiable for Google. For example, Google explains the following about certain cookies that it uses:

a. "[C]ookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time."[9]

b. "Most people who use Google services have a preferences cookie called 'NID' in their browsers. When you visit a Google service, the browser sends this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember your preferences and other information[.]"[10]

c. "We use cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, we use such cookies to remember your most recent searches, your previous interactions with an advertiser's ads or search results, and your visits to an advertiser's website. This helps us to show you customized ads on Google."[11]

d. "We also use one or more cookies for advertising we serve across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. We use other cookies with names

---

[9] *Privacy & Terms, Types of Cookies Used by Google*, Google, http://web.archive.org/web/20210916060858/https:/policies.google.com/technologies/cookies?hl=en-US (archived from September 16, 2021).

[10] *Privacy & Terms, Types of Cookies Used by Google*, Google, http://web.archive.org/web/20210101020222/https:/policies.google.com/technologies/cookies?hl=en-US (archived from January 1, 2021).

[11] *Id.*

> such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show you more relevant ads."[12]

83. Google warns web-developers that Google marketing tools are not appropriate for every type of website or webpage, including health-related webpages and websites.

84. Google warns developers in its Personalized Advertising policies page that "Health in personalized advertising" is a "Prohibited category" for Google's personalized advertising tools. Specifically, Google's advertising policies page states:[13]

> We take user privacy very seriously, and we also expect advertisers to respect user privacy. These policies define how advertisers are allowed to collect user data and use it for personalized advertising. They apply to advertisers using targeting features, including remarketing, affinity audiences, custom affinity audiences, in-market audiences, similar audiences, demographic and location targeting, and keyword contextual targeting. …
>
> You aren't allowed to do the following:

⊗ Collect information related to sensitive interest categories (see Personalized advertising policy principles below for more about sensitive interest categories)

85. Google further states that "[a]dvertisers can't use sensitive interest categories to target ads or to promote advertisers' products or services."[14] "Health" is one such "[p]rohibited categor[y]" that Google states "can't be used by advertisers to targets ads to users or promote advertisers' products or services."

---

[12] *Id.*

[13] *Advertising Policies Help, Personalized Advertising*, Google, http://web.archive.org/web/20191031223446/https://support.google.com/adspolicy/answer/143465?hl=en (archived from October 31, 2019).

[14] *Id.*

Health in personalized advertising

Personal health conditions, health issues related to intimate body parts or functions, and invasive medical procedures. This also includes treatments for health conditions and intimate bodily health issues.

- **Examples**: treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, over-the-counter medications for yeast infections, information about how to support your autistic child

Health content includes:

- physical or mental health conditions, including diseases, chronic conditions, and sexual health
- health condition-related services or procedures
- products for treating or managing health conditions, including over-the-counter medications for health conditions and medical devices
- long or short-term health issues associated with intimate body parts or functions, including genital, bowel, or urinary functions
- invasive medical procedures, including cosmetic surgery
- disabilities, even when content is oriented toward the user's primary caretaker

86. Google provides instructions for web developers to anonymize IP addresses when they use Google Analytics.[15] Google explains that the IP anonymization feature "is designed to help site owners comply with their own privacy policies or, in some countries, recommendations from local data protection authorities, which may prevent the storage of full IP address information."[16] The Google IP anonymization instructions tell web developers to add a parameter called 'aip' in their Google Analytics source code. When 'aip' ("anonymize IP") is turned on, it will be reported to Google Analytics in a GET request with the following: '&aip=1'.[17]

87. Upon information and belief, Defendant does not use Google's IP anonymization tool with Google Analytics. As a result, Defendant's use of Google Analytics is not anonymous, even when no cookies are involved in the re-direction of a patient's communication.

[15] *Analytics Help, IP Anonymization (or IP Masking) in Universal Analytics*, Google, https://support.google.com/analytics/answer/2763052?hl=en
[16] *Id.*
[17] *Id.*

88. Defendant deploys Google tracking tools on nearly every page on its web properties, including within the patient portal, thereby causing disclosure of communications exchanged with patients to be re-directed to Google.

Facebook

89. Facebook operates the world's largest social media company.

90. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers including IP addresses and cookie identifiers.

91. Facebook also tracks non-users across the web through its widespread Internet marketing products and source code.

92. Facebook's revenue is derived almost entirely from selling targeted advertising to Facebook users on Facebook.com and to all Internet users on non-Facebook sites that integrate Facebook marketing source code on their websites.

93. The Facebook Tracking Pixel is an invisible 1x1 web bug that Facebook makes available to web-developers to help developers track Facebook and other ad-driven activity on their website. Facebook warns developers that the Facebook Pixel is a personal identifier because it "relies on Facebook cookies, which enable [Facebook] to match your website visitors to their respective Facebook User accounts."

Implementation

The Facebook pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. It relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager and Analytics dashboard, so you use the data to analyze your website's conversion flows and optimize your ad campaigns.

94. Facebook recommends that the pixel code be placed early in the source code for any given webpage or website to ensure that the user will be tracked:

> **Installing The Pixel**
>
> To install the pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.
>
> Placing the code within your <head> tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

95. Defendant installed the Facebook Tracking Pixel to personally identify patients who click to log-in to the Defendant's patient portal at www.bjc.org.

96. When a patient clicks the "Login to MyChart" button at www.bjc.org, Defendants use the patient's personal identifiers by causing the identifiers to be transmitted to Facebook attached to the fact that the patient has exchanged a communication to log-in to the My Chart patient portal:

Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.bjc.org/
rl	https://doctors.bjc.org/
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"my-chart-button","destination":"https://www.bjc.org/For-Patients-Visitors/MyChart","id":"","imageUrl":"","innerText":"MyChart","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]	MyChart
cd[formFeatures]	[{"id":"StylesheetManager_TSSM","name":"StylesheetManager_TSSM","tag":"input","inputType":"hidden","valueMeaning":"empty"},{"id":"ScriptManager_TSM","name":"ScriptManager
cd[pageFeatures]	{"title":"\n\tBJC HealthCare | St. Louis, MO\n"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.62
r	stable
a	tmSimo-GTM-WebTemplate
ec	2
o	30
fbp	fb.[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
exp	p0
rqm	formPOST

97. The specific identifiers that Defendant uses to help Facebook acquire and record patient communications upon the My Chart Login click include the patient's IP address and cookie values, including first party cookies Defendant shares with Facebook via cookie synching.

98. Through the source code deployed by Defendant, the cookies that it uses to help Facebook identify patients include but are not necessarily limited to cookies named: c_user, datr, fr, and fbp.

99. The c_user cookie is a means of identification for Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

100. An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) clicking on their mouse, (3) selecting 'View page source,' (4) executing a control-F function for "fb://profile," and (5) copying the number value that appears after "fb://profile" in the page source code of the target Facebook user's page.

101. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. For example, the c_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

102. The datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every

datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

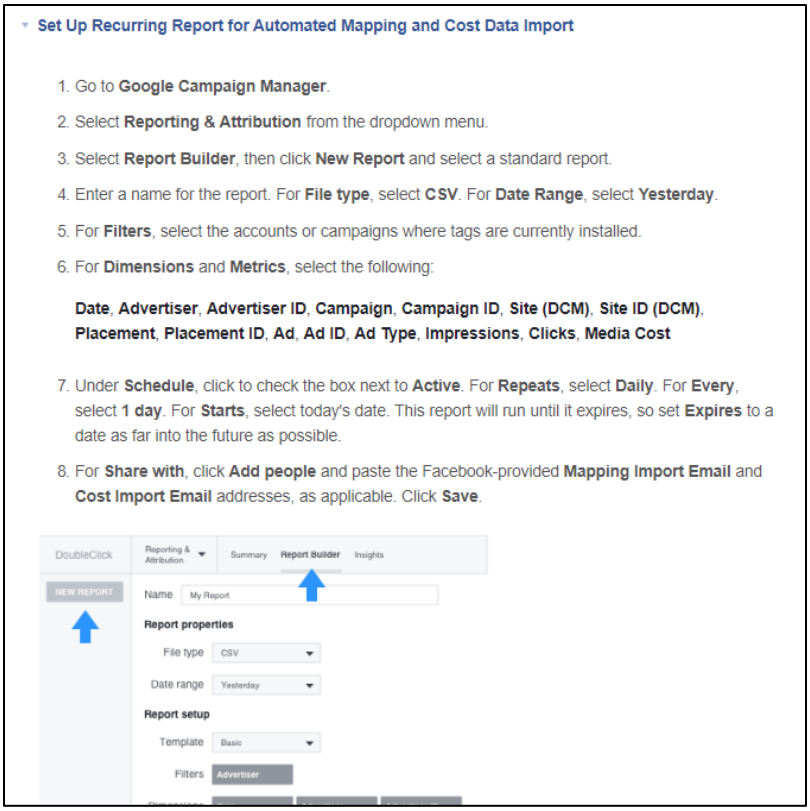
103. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[18]

104. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with BJC's use of the Facebook Tracking Pixel program. The fbp cookie emanates from Defendant's web properties as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy.

105. Facebook instructs developers on how to set-up their Google Campaign Manager to send automated regularly scheduled reports to Facebook:[19]

[18] *See* Gunes Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel, *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* (March 27, 2015) (available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf).

[19] *Google Campaign Manager (DoubleClick Campaign Manager)*, Meta, https://www.facebook.com/business/help/565734646951134 (last visited July 15, 2022).



106. In the absence of formal discovery and access to Defendant's Google and Facebook marketing accounts, it is impossible to know whether and how much data is disclosed to Facebook through this method.

TheTradeDesk

107. TheTradeDesk is an online advertising company that "helps advertisers and their advertising agencies manage digital advertising campaigns across many channels, such as websites, apps, audio, smart tvs, and other video."[20]

[20] *Privacy and The Trade Desk Platform*, theTradeDesk, https://www.thetradedesk.com/general/privacy (last updated January 20, 2022).

108. TheTradeDesk admits that its marketing platform collets the following categories of information for "up to 18 months before [TheTradeDesk] aggregate[s] it":

The data our Platform collects and processes:	Pseudonymous data such as: • unique cookie and device identifiers • mobile device advertising identifiers • IP addresses • web browsing history from advertising impressions we see • interest information inferred by us from web browsing history • interest information stored and/or used on the Platform by clients and partners • location information • browser and device type, version and settings

109. As described by theTradeDesk, the "pseudonymous" data it collects is personally identifiable information under HIPAA.

110. Defendants deploy theTradeDesk tracking tools and makes disclosures to theTradeDesk via adsrvr.org.

SiteScout

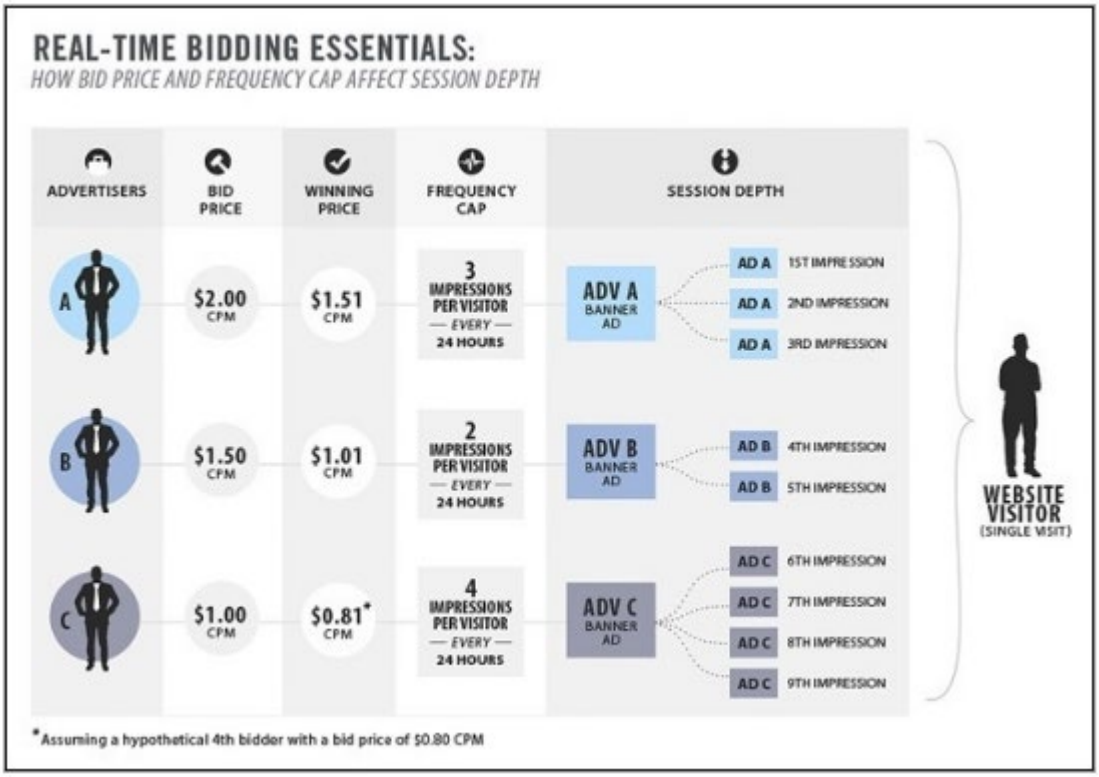
111. Defendants also deploy the SiteScout pixel across its web properties.

112. SiteScout describes itself as a "self-serve ad buying platform that makes it easy for marketers to buy programmatic ads across all devices and channels."[21] SiteScout facilitates its ad buying platform through "real-time bidding" ["RTB"] technology which "enables publishers (website owners) to sell advertising inventory through an ad exchange platform on an impression-by-impression basis as each impression becomes available on a publisher's website (i.e., in real time)."[22]

[21] SiteScout, [@SiteScout], https://twitter.com/sitescout.

[22] *The Basics of SiteScout RTB*, SiteScout, https://support.sitescout.com/getting_started/sitescout_basics.htm?tocpath=Help%20Topics%7CGetting%20Started%7C_____1 (last visited July 15, 2022).

113. "As the name implies, RTB operates on an auction model. You set the max bid (CPM) that you will pay for a placement and win impressions at $0.01 above the next highest bidder. Here is an illustration:



If 'Advertiser A' bids $2.00 CPM and 'Advertiser B' bids $1.50 CPM, 'Advertiser A' will win the impression at $1.51 CPM (Or to put it more accurately, $0.00101 for that specific impression.)" *Id*.

114. SiteScout explains exactly how the RTB targeting technology—which Defendant deployed on its web properties—works:

> In the milliseconds before ads are served, *we are given a ton of details about the user who is about to view the upcoming ad. From geographic location to browser and device information, we have access to an abundance of data that is used for targeting.* Within our platform, you can specify most of this targeting data as an audience filter for your campaigns. This way you can ensure the right people will be viewing your ad.

> In short, every impression is analyzed individually based on its characteristics and bid on accordingly if it matches an advertiser's targeting criteria.

Id.

115. SiteScout also uses "contextual targeting" to serve advertisements, which it describes as:

> Contextual targeting allows advertisers to only place their ads on pages that meet their topical criteria. For example, advertisers can choose to have their ads served only on pages that match chosen topical categories such as "Real Estate::Buying/Selling Homes" or "Fashion::Accessories", depending on the subject matter and target demographic of their campaign.
>
> ***
>
> Whenever an impression comes into the system, the URL of the impression is analyzed. Once the content of the URL is evaluated, it returns with several categorizations, along with a number that indicates the relevancy score of each attributed category.
>
> For example, a page containing a news article that discusses a national election might have the following categorizations attributed to it:
>
> - Law, Gov't, & Politics: Politics = 96 (high)
> - Business: Government = 85 (high)
> - Personal Finance: Retirement Planning = 55 (moderate)
> - Real Estate: Buying/Selling Homes = 34 (low)
> - Society: Senior Living = 21 (low)

Contextual Targeting, SiteScout, https://support.sitescout.com/platform_integrations/contextual_targeting.htm?tocpath=Help%20Topics%7CPlatform%20Integrations%7C_____2 (last visited July 15, 2022).

116. Real time bidding platforms, such as those used by SiteScout, constitute the sale of patient data in violation of Defendant's legal and ethical obligations, as well as its privacy promises.

What Happens When a Patient Communicates with Defendants at Their Web Properties

117. Fiddler is a software application used by web developers to test how their various applications and source codes operate. By using Fiddler, one can also capture and record

communications and other data transmissions that flow to and from a web-browser over the Internet. The following is derived from use of Fiddler in connection with the BJCHealth.com web property.

118. When a patient first visits the bjc.org homepage, the source code that BJC causes personally identifiable patient data to be transmitted and the contents of patient communications to be re-direct to third parties connected to the fact that the patient is present at the BJC property.

119. A patient might first use the tab provided by BJC to identify themselves as a patient for purposes of using the BJC web property:

120. When a patient clicks the tab to receive "Virtual Care," BJC causes the transmission of the patient's personally identifiable data and re-directs the content of the patient's click of the "Virtual Care" button to Facebook.

121. Fiddler shows the following data is transmitted to Facebook through a fake "formPOST" request caused by BJC's source code.

Body

Name	Value
a	tmSimo-GTM-WebTemplate
cd[buttonFeatures]	{"classList":"button-blue","destination":"https://scheduling.bjc.org/virtual-care-schedule?_ga=[redacted]
cd[buttonText]	Schedule Telehealth Visit
cd[formFeatures]	[{"id":"StylesheetManager_TSSM","name":"StylesheetManager_TSSM","tag":"input","inputType":"hidden","valueMeaning":"empty"},{"id":"ScriptManager_TSM",
cd[pageFeatures]	{"title":"\n\tVirtual Care | Telehealth visits with a BJC Doctor or Nurse\n"}
cd[parameters]	[]
coo	false
dl	https://www.bjc.org/Virtual-Care
ec	2
es	automatic
ev	SubscribedButtonClick
exp	p1
fbp	fb.[redacted]
id	[redacted]
if	false
it	[redacted]
o	30
r	stable
rl	
rqm	formPOST
sh	1080
sw	1920
tm	3
ts	[redacted]
v	2.9.62

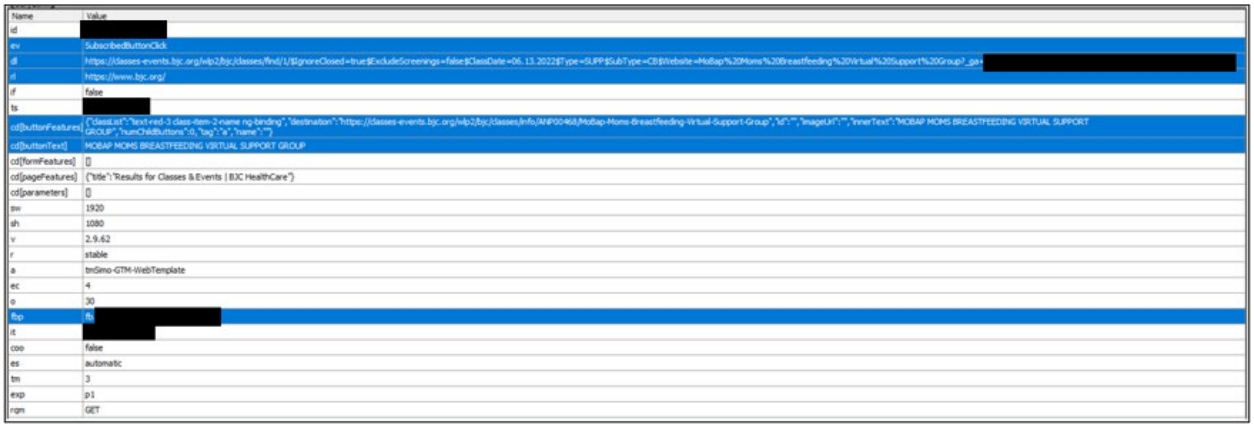
This chart shows disclosure to Facebook that the patient engaged in an event ('ev') labeled "SubscribedButtonClick," that the "buttonText" was "Schedule Telehealth Visit," that the button was clicked from https://www.bjc.org/Virtual-Care, and the details of the first-party fbp cookie assigned by BJC. In addition, BJC transmits the user's unique Google Analytics cookie identifier, _ga," to Facebook.

122. BJC causes multiple data transmissions to be made to Facebook before the data is sent to BJC.

123. BJC causes similar data transmissions to be sent to Facebook with every communication that a patient sends at its www.bjc.org web property. For example, when a patient sends a communication seeking more information on "reproductive care" (or any other search), BJC causes data transmissions to be made to third parties, including Google, that include personally identifiable patient data and the content of the patient's re-directed communication.

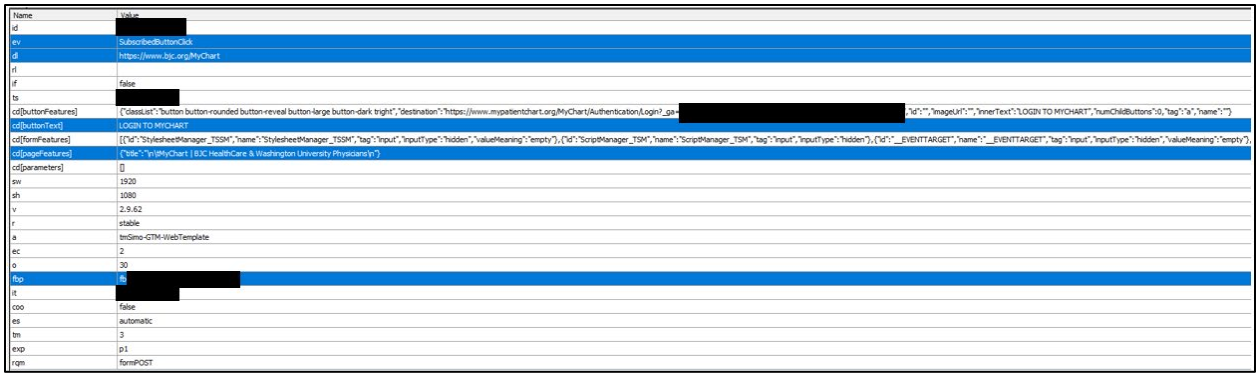
124. Immediately upon a patient sending the "reproductive care" search communication to Defendant, the source code triggers over 100 separate contemporaneous data transmissions containing personally identifiable patient data and the content of the patient's communication to third parties, including Facebook, Google, SiteScout, The TradeDesk, and Invoca.

125. An example transmission to Facebook includes the following:



This shows that the patient has engaged in a "SubscribedButtonClick," that the text of the button was "MOBAP MOMS BREASTFEEDING VIRTUAL SUPPORT GROUP," that the user was searching for "ClassDate=06.13.2022," the user asked that the search to exclude closed classes, the patient's Google Analytics identifier, and the patient's Facebook Pixel identifier.

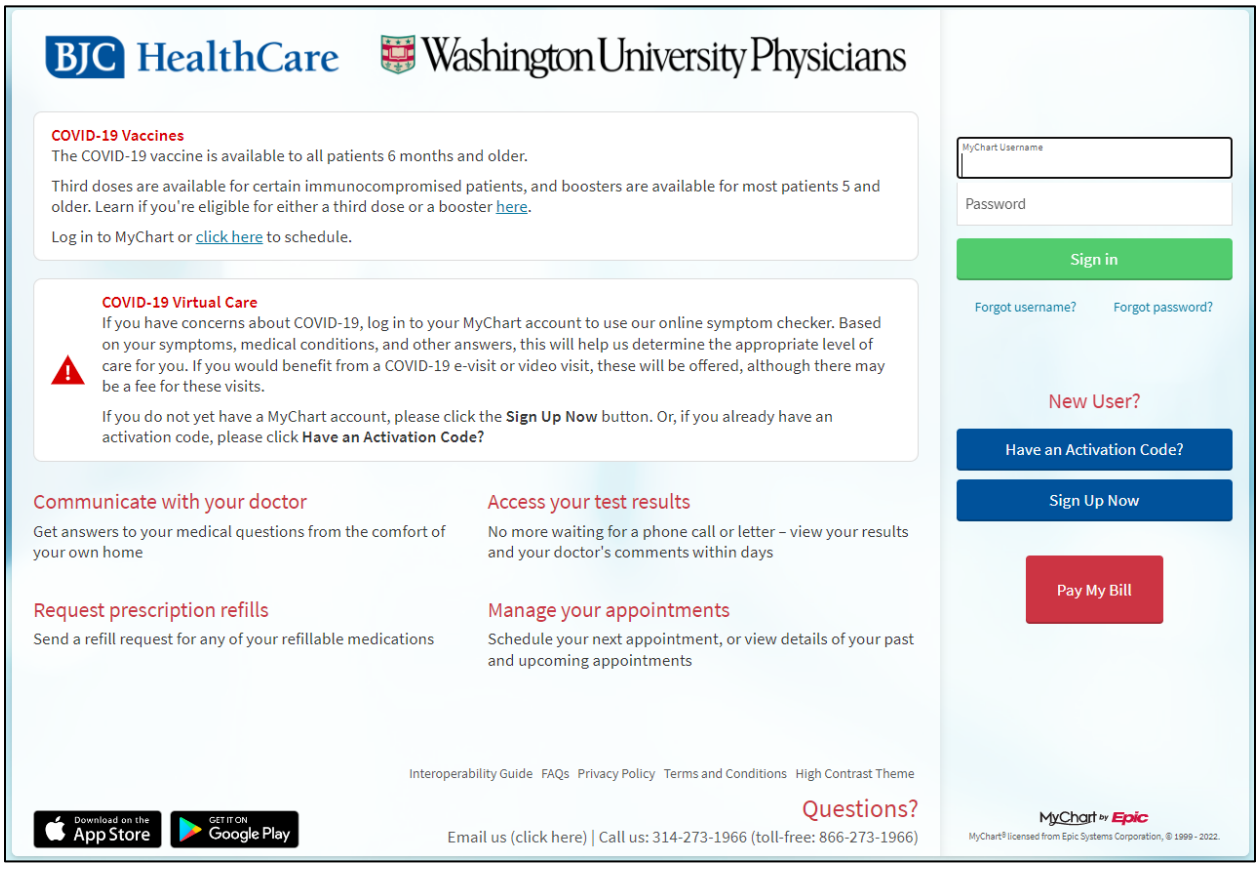
126. If the patient continues his or her browsing session to login to the patient portal, Defendant transmits substantially similar information, including the patient's Google and Facebook identifiers:



Name	Value
id	[redacted]
ev	SubscribedButtonClick
dl	https://www.bjc.org/MyChart
rl	
if	false
ts	[redacted]
cd[buttonFeatures]	{"classList":"button button-rounded button-reveal button-large button-dark tright","destination":"https://www.mypatientchart.org/MyChart/Authentication/Login?_ga=[redacted]","id":"","imageUrl":"","innerText":"LOGIN TO MYCHART","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]	LOGIN TO MYCHART
cd[formFeatures]	[{"id":"StylesheetManager_TSSM","name":"StylesheetManager_TSSM","tag":"input","inputType":"hidden","valueMeaning":"empty"},{"id":"ScriptManager_TSM","name":"ScriptManager_TSM","tag":"input","inputType":"hidden"},{"id":"__EVENTTARGET","name":"__EVENTTARGET","tag":"input","inputType":"hidden","valueMeaning":"empty"},
cd[pageFeatures]	{"title":"\n\tMyChart | BJC HealthCare & Washington University Physicians\n"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.62
r	stable
a	tmSmo-GTM-WebTemplate
ec	2
o	30
fbp	fb[redacted]
it	[redacted]
coo	false
es	automatic
tm	3
exp	p1
rqm	formPOST

This shows BJC has caused disclosure that the patient has engaged in a "SubscribedButtonClick," that the text of the button was "LOGIN TO MYCHART," that the user was visiting a "BJC Healthcare & Washington University Physicians" web property, the patient's Google Analytics identifier, and the patient's Facebook Pixel identifier.

127. However, all of these transmission are hidden from the patient. Instead, the patient only sees the following page rendered, without an indication of third party disclosures:



128. Regardless of the next link a patient clicks to continue its communication with BJC at the BJC web-property, the source code purposefully deployed by BJC will cause transmission of their personally identifiable patient data and simultaneously re-direct the specific contents of their communication to Facebook, Google, theTradeDesk, SiteScout, and Invoca.

THE VALUE OF THE PERSONALLY IDENTIFIABLE DATA AND COMMUNICATIONS BJC USES AND DISCLOSES WITHOUT PATIENTS' KNOWLEDGE, CONSENT, AUTHORIZATION, OR FURTHER ACTION

129. The value of data that companies like Facebook and Google extract from people who use the Internet is well understood and generally accepted in the e-commerce industry.

130. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

131. The cash value of Internet users' personal information can be quantified. In a 2015 study by the Ponemon Institute, researchers determined the value that American Internet users place on their "health condition" as more valuable than any other piece of data about them, with a minimum value of $82.90.[23]

132. Medical information derived from medical providers garner even more value from the fact that it is not available to third party data marketing companies because of strict restrictions

[23] Ponemon Institute, Privacy and Security in a Connected Life: A Study of US Consumers, March 2015, available at https://vdocuments.site/privacy-and-security-in-a-connected-life-protect-personal-information-from-being.html?page=1.

on provider disclosures under HIPAA, state laws, and provider standards, including the Hippocratic oath.

133. Even with restrictions on the disclosure of personally identifiable health information, a robust market exists for the trade of de-identified health data.[24]

BJC'S DUTIES OF CONFIDENTIALITY

BJC's Duties Under Federal Law

134. Under federal law, a health care provider may not disclose personally identifiable information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

135. Guidance from the United States Department of Health and Human Services instructs health care providers that patient status alone is protected by HIPAA.

136. In Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. … If such information was listed with health condition, health care provision or payment data, *such as an indication that the individual was treated at a certain clinic*, then this information would be PHI.

[24] *See* Adam Tanner, *How Data Brokers Make Money Off Your Medical Records,* Scientific American, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/ (February 1, 2016); Sam Thielman, *Your Private Medical Data is for Sale – and It's Driving a Business Worth Billions*, The Guardian, https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns (January 10, 2017); Adam Tanner, *The Hidden Global Trade in Patient Medical Data,* YaleGlobal Online, https://archive-yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data (last visited July 15, 2022).

(emphasis added).[25]

137. BJC has interpreted the HIPAA rules to protect patient status. On May 27, 2022, BJC placed a notice banner on its homepage notifying patients that a "security incident" had occurred which resulted in the unauthorized access of "contained some patients' information, which may have included names, dates of birth, medical record numbers, and clinical information, such as dates of service, diagnoses, provider names, and/or treatment locations." BJC self-reported the breach to Health and Human Services.

138. In its guidance for Marketing, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. Emphasis added.[26]

Ancient and Modern Industry Standards of Patient Confidentiality

139. A medical provider's duty of confidentiality to patients is ancient in origin.

140. The original Hippocratic Oath, circa 400 B.C., provided that physicians must pledge, "What I may see or hear in the course of treatment or even outside of the treatment in

---

[25] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,* at 5, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (November 26, 2012).

[26] *Marketing*, at 1-2, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (April 3, 2003).

regard to the life of man, which on no account must be spread abroad, I will keep to myself holding such things shameful to be spoken about."[27]

141. The modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[28]

142. A medical provider's duty of confidentiality to patients still applies today. In fact, the American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

143. The Missouri Supreme Court has explained that, "The AMA Principles of Medical Ethics provides, 'The physician should not reveal confidential communications of information without the express consent of the patient, unless required to do so by law."

144. AMA Code of Medical Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust. Patient privacy encompasses a number of aspects, including … personal data (informational privacy)[.] … *Physicians must seek to protect patient privacy in all settings to the greatest extent possible* and should: (a) Minimize intrusion on privacy when the patient's privacy must be balanced against other factors. (b) Inform the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware. [and] (c) Be mindful that individual patients may have special concerns about privacy in any or all of these areas.

145. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of a patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship.

---

[27] As recited in *Brandt v. Medical Defense Associates*, 856 S.W.2d 667, 671, n. 1 (Mo. 1993)

[28] LOUIS LASAGNE, HIPPOCRATIC OATH—MODERN VERSION, *at* http://www.pbs.org/wgbh/nova/doctors/oath_modern.html.

> Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.[29]

146. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> *Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.* Physicians who collect or store patient information electronically … must: … (c) release patient information only in keeping with ethics guidelines for confidentiality.

(emphasis added).[30]

Consumer Expectations of Patient Privacy

147. Confidentiality is a cardinal rule of the provider-patient relationship.

148. Patients are aware of their medical provider's duty of confidentiality, and, as a result, have an objectively reasonable expectation that their health care providers will not share their personally identifiable data and communications with third parties in the absence of authorization for any purpose that is not directly related or beneficial to the patient's care.

149. A recent national survey from CVS-Aetna revealed that "[p]rivacy and data security lead patients' concerns in the changing health environment." Eighty percent of survey respondents "indicated that privacy was a top concern regarding their health care, while 76 percent of individuals felt the same high level of concern for their data security." Both totals are higher than the 73 percent of consumer who indicate that cost is important to their care.

---

[29] *Code of Medical Ethics Opinion 3.2.4*, AMA, https://www.ama-assn.org/delivering-care/ethics/access-medical-records-data-collection-companies (last visited July 15, 2022).

[30] *Code of Medical Ethics Opinion 3.3.2*, AMA, Conf https://www.ama-assn.org/delivering-care/ethics/confidentiality-electronic-medical-records (last visited July 15, 2022).

BJC Assures Patients That It Protects Their Personally Identifiable Information

150. Patients' reasonable expectations of privacy are further supported by express and implied promises by BJC.

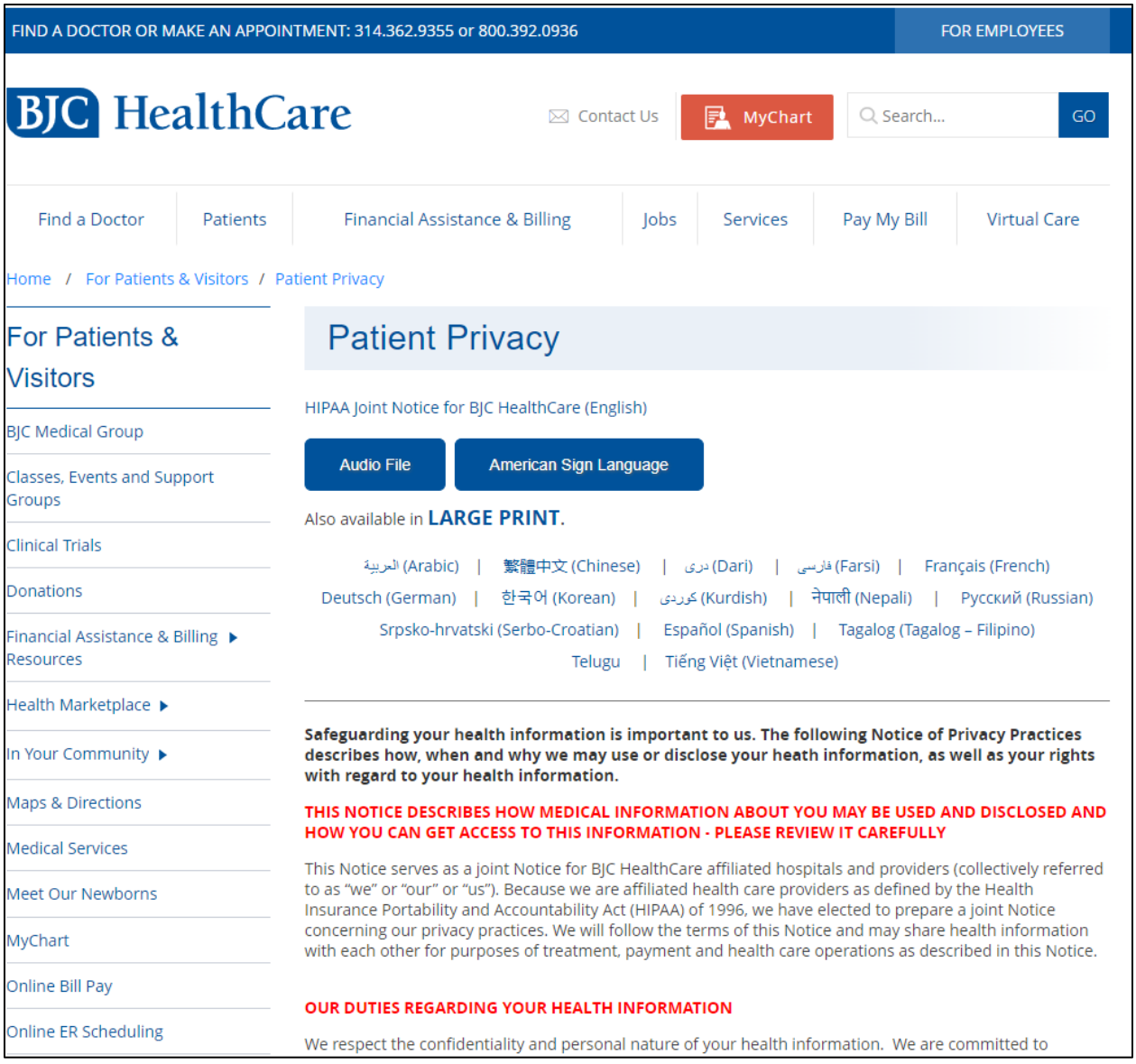
151. By law, BJC is required to provide patients with a copy of its HIPAA Notice of Privacy Practices, and to display such notice at its properties, including its web property.

152. To comply with the requirement of posting the HIPAA notice on its web-property, the BJC web-property contains a sub-footer link to "Patient Privacy."

153. The Privacy link appears at the bottom of each page at www.bjc.org.

154. The very term "Privacy Policy" is deceptive. Research has consistently shown that a majority of Americans who see that a website has a "Privacy Policy" falsely believe that the company with the policy cannot disclose information about them without their consent.

155. By clicking on the "Patient Privacy" link, a patient is directed to a page contains BJC's Joint Notice for BJC HealthCare, and appears as:



156. By taking such action of linking the Privacy link to the HIPAA Notice of Privacy Practices, BJC gives patients the impression that it treats their communications at its web property with the same confidentiality that it treats patient communications at its physical properties.

157. As a matter of law, there is no exception in HIPAA for communications between patients and providers that occur over the Internet.

158. BJC's Notice of Privacy Practices promises the following:

a. "We respect the confidentiality and personal nature of your health information. We are committed to protecting your health information and to informing you of your rights regarding such information."

b. "We are required by law to protect the privacy of your protected health information, to provide you with notice of these legal duties and to notify you following a breach of unsecured protected health information."

c. "After removing direct identifying information (such as your name, address and Social Security number) from the health information, we may use your health information for research, public health activities or other health care operations (such as business planning). While only limited identifying information will be used, we will also obtain certain assurances from the recipient of such health information that they will safeguard the information and only use and disclose the information for limited purposes."

d. "We will not engage in disclosures that constitute a sale of your health information without your written authorization. A sale of protected health information occurs when we, or someone we contract with directly or indirectly, receive payment in exchange for your protected health information."

e. "We will not use or disclose your protected health information for marketing purposes without your written authorization. Marketing is defined as receipt of payment from a third party for communicating with you about a product or service marketed by the third party."

Patient Privacy, BJC HealthCare, https://www.bjc.org/For-Patients-Visitors/Patient-Privacy (last visited July 15, 2022).

159. The design of the BJC website with its HIPAA Joint Notice of Privacy Practices and the statements contained within it are false, deceptive, and misleading. As described herein, BJC routinely causes personally identifiable patient data and the content of their communications to be transmitted and re-directed to third parties for marketing purposes.

160. The footer on the BJC web properties also includes a hyperlink for "Our Policies," which sends the patient to a page titled "BJC HealthCare Web and Internet Policies":

BJC HealthCare Web and Internet Policies

Terms of Use
BJC HealthCare is providing information and services on this website as a benefit to our users. The information and services on this website are provided solely for general illustration, educational and resource provision purposes. Such information and services are not intended to be specific medical, health, business or other professional advice or direction. If you have specific questions regarding your health or health status, contact your physician or other health care provider. Neither BJC HealthCare nor its information contributors make any express or implied representations or warranties about the completeness or accuracy of this information and these services for any purpose, or the suitability of this information or these services for any particular use.

This website also enables users to obtain information on the services, events and materials offered, happening or available through BJC HealthCare and its facilities, including publications and educational programs, current news, certain BJC HealthCare documents, lists of health-related websites, and other information relevant to purposes of this website.

This website may include links providing direct access to other websites. However, BJC HealthCare takes no responsibility for the content or information contained on those other websites, and does not exert any editorial, monitoring or other control over those other websites and, therefore, does not assume any liability for those websites or their content. BJC HealthCare reserves the right to remove any link from this website for any or no reason. The existence of any particular link is simply intended to imply potential interest to users of this website.

Certain areas of the website may allow for the posting or exchange of information among and between users. Users who submit or post information to this website grant BJC HealthCare the authority and right to use any submission in any way, and by such submissions warrant and represent to BJC HealthCare that such submissions are not in violation of United States copyright or other laws. In addition, BJC HealthCare reserves the right to review, edit or delete any information (including, without limitation, those that appear to be inappropriate for the intended purpose).

All images, text and other materials posted on this website are subject to copyrights owned by BJC HealthCare or other individuals or entities, and are protected by United States copyright laws. Any reproduction, retransmission, distribution or republication of all or part of any images, text programs, and other materials found on this website is expressly prohibited, unless BJC HealthCare or the copyright owner of the material has expressly granted its prior written consent. All other rights reserved. This website is intended to be maintained in a manner consistent with United States copyright laws. Accordingly, users should not submit copyrighted material to this website unless the copyright owner of the material has expressly granted its prior written consent to such submission.

All trademarks, service marks and logos referred to or appearing on this website are the property of their respective owners. The names, trademarks, service marks and logos of BJC HealthCare appearing on this website may not be used in any advertising or publicity, or otherwise to indicate sponsorship of or affiliation with any product or service, without BJC HealthCare's prior express written permission.

Privacy Statement
BJC HealthCare has created this statement to demonstrate its commitment to your privacy. This statement explains BJC HealthCare's information-gathering and dissemination practices for this website.

A typical visit to our website does not require a user to submit personal information. However, if you send us an e-mail with your contact information, we will inquire if we may send information to you. If you reply in the affirmative, your name and contact information will be entered into a database for potential use in a future mailing or e-mail distribution.

Information you submit may be routinely shared with the Washington University School of Medicine, if you are looking for a physician referral. Other than this organization, we will only forward your personal information to organizations working on our behalf. We urge you not to provide any confidential information about you or your health to us via electronic communication. If you do so, it is at your own risk. Although we attempt to maintain our computer network in a secure manner to protect the content of your messages, we cannot provide absolute assurance that the contents of your e-mail will not become accessible to individuals or entities that are not authorized to access your information.

The Cookie
It is our desire that each online visitor experience an optimum experience in finding medical information and learning about BJC HealthCare services. In working toward that goal, we count our visitors and keep track of where our visitors go throughout the website. To do this, we must use software called a "cookie." The "cookie" maintains numbers in aggregate form, and does not obtain personal information about our visitors. This information helps us know what sections of our website are visited frequently, so we can enhance those sections and ensure they're up-to-date. None of the research we conduct is shared with companies unrelated to BJC HealthCare.

BJC HealthCare Web and Internet Policies, BJC HealthCare, https://www.bjc.org/Our-Policies (last visited July 15, 2022).

161. The "Web and Internet Policies" page does not disclose BJC's secret deployment of third-party technology on its web properties, nor the disclosure of patient PII and communications to third parties.

162. In fact, BJC's policy states the opposite. BJC says that it "created this statement to demonstrate its commitment to your privacy. This statement explains BJC HealthCare's information-gathering and dissemination practices for this website." It further falsely claims that "A typical visit to our website does not require a user to submit personal information."

163. These statements are demonstrably false in light of BJC's secret disclosure of patient information and communications to numerous third parties, including Facebook, Google, SiteScout, TheTradeDesk, and Invoca.

164. Similarly, BJC's cookie policy, specifically, is demonstrably false. It states:

The Cookie
It is our desire that each online visitor experience an optimum experience in finding medical information and learning about BJC HealthCare services. In working toward that goal, we count our visitors and keep track of where our visitors go throughout the website. To do this, we must use software called a "cookie." The "cookie" maintains numbers in aggregate form, and does not obtain personal information about our visitors. This information helps us know what sections of our website are visited frequently, so we can enhance those sections and ensure they're up-to-date. None of the research we conduct is shared with companies unrelated to BJC HealthCare.

165. This statement is false and misleading in several ways, including:

a. BJC states it "must use software called a 'cookie'" when, in fact, third party cookies are not necessary for the functionality of its web properties;

b. BJC states that it "does not obtain personal information about our visitors" through the use of cookies when, in fact, the transmission of these unique cookie values and identifiers constitutes PHI under HIPAA,

c. BJC states that "None of the research [with cookies] we conduct is shared with companies unrelated to BJC HealthCare" when, in fact, BJC transmits patient personally identifiable information and communications to

numerous entities outside of BJC including Facebook, Google, SiteScout, Invoca, and TheTradeDesk.

166. A health care provider's duty of confidentiality cannot be waived via an inconspicuous, unenforceable browse-wrap privacy policy (like that used by BJC in its footer) regardless of the contents of the policy. This is especially true where the browse-wrap policy is not provided via effective notice but is only viewable if a user scrolls through multiple separate screens of content, and then is displayed in light blue font hidden on a medium blue background.

167. In the absence of effective notice, browse-wrap statements do not create enforceable contracts against consumers.

168. The vast majority of Internet users do not read privacy policies or website terms of use. One study found that only between 0.05 to 0.22 percent of online shoppers (or 1 to 2 of every 1,000 shoppers) access online agreements—even click- or scroll-wrap agreements rather than browse-wrap agreements.[31]

169. Chief Justice John Roberts admits he does not read purported online agreements.[32]

170. The cost of reading all privacy policies a consumer encounters is high. It would take an average American consumer between 181 to 304 hours per year to read the purported privacy policies of websites with which they interact.[33] This would require a consumer to devote an estimated 40 minutes per day to reading privacy policies. The time-money calculation for this

[31] Yannis Bakos, Florencia Marotta-Wurgler and David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts*, 43 J. LEGAL STUD. 1, 1 (2014).
[32] Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA Journal (Oct. 20, 2010) ("Answering a student question, Roberts admitted he doesn't usually read the computer jargon that is a condition of accessing websites.")
[33] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 563 (2008).

effort is between $2,553 to $5,038 per year per consumer for a collective national cost of $559.7 billion to $1.1 trillion per year.

171. Regardless, it is reasonable for a patient to assume that their health care providers' privacy policies are consistent with their providers' duties of confidentiality and patient expectations of privacy.

172. Plaintiffs did not read BJC's purported Terms and Conditions or purported Website Privacy Policy.

CLASS ACTION ALLEGATIONS

173. Plaintiff re-alleges and incorporates by reference the allegations set forth above.

174. Pursuant to Missouri Supreme Court Rule 52.08, Plaintiffs bring this class action and seeks certification of the claims on behalf of the following class:

> During the fullest period allowed by law, all Missouri residents who are, or were, patients of BJC or any of its affiliates and accessed BJC's MyChart patient portal that causes transmission of personally identifiable data and communications to be made to third-parties.

175. Plaintiffs reserve the right to amend the Class definition if further investigation, discovery, or litigation indicates that the definition should be expanded, narrowed, or otherwise modified.

176. This action has been brought and may be maintained as a class action under Missouri Supreme Court Rule 52.08.

177. Numerosity – Class members are so numerous that their individual joinder is impracticable. The precise number of Class members and their identities are unknown to Plaintiffs at this time but will be determined through discovery through the records of the Defendant.

178. Existence and Predominance of Common Questions of Law and Fact – Common questions of law and fact exist and predominate over questions affecting only individual Class

members. These common legal and factual questions, each of which may also be certified individually under Rule 52.08(c)(4), include the following:

a. Whether Defendant's practices relating to disclosures of Plaintiffs' and patient Class Members' personally identifiable data and communications to third parties were intentional;

b. Whether Defendant profited from disclosures to the third parties;

c. Whether Defendant's practices alleged herein were unfair, deceptive, and/or unlawful in any respect, thereby violations the Missouri Merchandising Practices Act;

d. Whether Defendant's practices constitute an unauthorized intrusion upon seclusion;

e. Whether Defendant's practices constitute breach of fiduciary duty of confidentiality;

f. Whether Defendant's actions violate sections §§569.095-.099, RSMo;

g. Whether Defendant's actions violation § 570.223, RSMo;

h. Whether Defendant's conduct harmed and continues to harm Plaintiffs and Class Members, and if so, the extent of the injury;

i. Whether and to what extent Plaintiffs and Class Members are entitled to damages and other monetary relief;

j. Whether and to what extent Plaintiffs and Class Members are entitled to equitable relief, including, but not limited to, a preliminary and/or permanent injunction; and

k. Whether and to what extent Plaintiffs and Class Members are entitled to attorney fees and costs.

179. Typicality – Plaintiffs' claims are typical of the claims of the Class and Plaintiffs have substantially the same interest in this matter as other Class Members. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of the other members of the Class. Plaintiffs' claims arise out of the same set of facts and conduct as all other Class Members. Plaintiffs and all Class Members are all Missouri residents who are or were patients of Defendant who used the Defendant's web-property set-up by Defendant for patients, and are victims of the Defendant's unauthorized disclosures to third-parties. All claims of the Plaintiffs and Class Members are based on Defendant's wrongful conduct and unauthorized disclosures.

180. Adequacy of Representation – Plaintiffs will fairly and adequately protect the interests of Class Members. Plaintiffs have retained competent counsel experienced in complex class action privacy litigation and Plaintiffs will prosecute this action vigorously. Plaintiffs have no interests adverse or antagonistic to those of the Class.

181. Superiority – A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are small compared with the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class Members, on an individual basis, to obtain effective redress for the wrongs done them. Furthermore, even if Class Members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By

contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

182. Additionally, the Class may be certified under Rule 52.08(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

c. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the Class Members as a whole.

COUNT I
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY
***Brandt v. Medical Defense Associates*, 856 S.W.2d 667 (Mo. 1993)**

183. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

184. BJC designed its web property at www.bjc.org for patients to exchange communications with BJC relating to providers, treatment, billing, conditions, and medical records.

185. BJC's web property links to a HIPAA notice that assures Plaintiffs and other patient Class Members that Defendant will protect the confidentiality of their data and communications and not use them for marketing purposes without express written authorization.

186. Defendant has a fiduciary duty not to disclose for marketing purposes information received from or sent to patients without a patient's express written authorization.

187. Defendant breached its fiduciary duty of confidentiality by intentionally deploying source code at its web property www.bjc.org that caused the transmission of personally identifiable patient data and the re-direction to Facebook, Google, theTradeDesk, and SiteScout of the contents of communications exchanged with BJC's own patients.

188. As a direct and proximate result of Defendant's breach of fiduciary duty of confidentiality, Plaintiffs and patient Class Members were damaged by Defendant's breach in that:

a. Defendant harmed Plaintiffs and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no more;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs and Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

f. Defendant's actions diminished the value of Plaintiffs and Class Members' personal information.

WHEREFORE, on behalf of himself and others, Plaintiffs pray for judgment against Defendant for an amount excess of $25,000 that is fair, just, and reasonable and for the costs expended herein, for post-judgment interest on said sums, and for such other relief as the Court deems just and proper.

COUNT II
INTRUSION UPON SECLUSION

189. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

190. Plaintiffs' communications with BJC constitute private conversations, matters, and data.

191. Plaintiffs and patient Class Members have a reasonable expectation that BJC would not disclose personally identifiable patient data and communications to third parties for marketing purposes without Plaintiffs and other patient Class members authorization, consent, knowledge, or any further action on the patient's part.

192. BJC, a health care provider, has a duty to keep personally identifiable patient data and communications confidential.

193. BJC expressly promised to maintain the confidentiality of personally identifiable patient data and communications in its HIPAA Notice of Privacy Practices and Web and Internet Policies.

194. BJC intruded upon Plaintiffs' seclusion by deploying source code that caused the transmission of Plaintiffs' personally identifiable data and the contents of communications he exchanged with his health care provider to third parties including Facebook, Google, theTradeDesk, and SiteScout.

195. Plaintiffs and patient Class Members did not authorize, consent, know about, or take any action to indicate consent to Defendant's conduct alleged herein.

196. BJC's conduct described herein was intentional.

197. BJC's conduct in disclosing Plaintiffs' information to third parties was and is highly offensive to a reasonable person.

198. As a direct and proximate result of Defendant's intrusion upon his seclusion, Plaintiffs and patient Class Members were damaged by Defendant's intrusion in that:

a. BJC harmed Plaintiffs' and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no more;

c. BJC eroded the essential confidential nature of the provider-patient relationship;

d. BJC took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included BJC's duty to maintain confidentiality; and

f. BJC's actions diminished the value of Plaintiffs and Class Members' personal information.

WHEREFORE, on behalf of himself and others, Plaintiffs pray judgment against Defendant for an amount excess of $25,000 that is fair, just, and reasonable and for the costs

expended herein, for post-judgment interest on said sums, and for such other relief as the Court deems just and proper.

COUNT III
VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT, RSMo. §§ 407.010, *et seq*.

199. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

200. The Missouri Merchandising Practices Act ("the Act") provides that "[t]he act, use or employment by any person of any deception . . . [or] unfair practice, or the concealment . . . of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce . . . is declared to be an unlawful practice." § 407.020.1, RSMo.

201. The enabling regulations for the Act define an "unfair practice" as conduct that (1) offends public policy; (2) is unethical, oppressive, and unscrupulous; (3) causes a risk of substantial injury to consumers; (4) was not in good faith; (5) is unconscionable; or (6) is unlawful. *See* 15 C.S.R. §§ 60-8.020, 60-8.040, & 60-8.090.

202. Under the Act, the term "merchandise" is broadly defined to include any services and intangibles. § 407.010.4, RSMo.

203. The Act authorizes private causes of action, and class actions. §§ 407.025.1; 407.025.2, RSMo.

204. Plaintiffs received and paid for health care services from Defendant.

205. Plaintiffs' payment to BJC for health care services was for household and personal purposes.

206. BJC's practice of disclosing Plaintiffs' personally identifiable data and re-directing his communications without his authorization, consent, or knowledge to third parties is an unfair practice within the meaning of the Act.

207. As a result of BJC violating the Act, Plaintiffs and others sustained an ascertainable loss of money when they overpaid for BJC's health care services.

208. Defendant's violations of the Act were willful and knowing.

209. As a direct and proximate result of BJC's intrusion upon his seclusion, Plaintiffs and patient Class Members were damaged by Defendant's intrusion in that:

a. BJC harmed Plaintiffs and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no more;

c. BJC eroded the essential confidential nature of the provider-patient relationship;

d. BJC took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs and Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included BJC's duty to maintain confidentiality; and

f. BJC's actions diminished the value of Plaintiffs and Class Members' personal information.

a. Plaintiffs and Class Members seek actual damages; a declaration that BJC's methods, acts and practices violate the Missouri Merchandising Practices Act; an injunction prohibiting Defendant from continuing to engage in such unlawful methods, acts, and practices;

restitution; rescission; disgorgement of all profits obtained from BJC's unlawful conduct; pre and post-judgment interest; and attorneys' fees and costs.

WHEREFORE, on behalf of himself and others, Plaintiffs pray judgment against Defendant for an amount excess of $25,000 that is fair, just, and reasonable and for the costs expended herein, for post-judgment interest on said sums, and for such other relief as the Court deems just and proper.

COUNT IV
FELONY COMPUTER CRIMES

210. Plaintiffs incorporate all preceding paragraphs as if set forth fully herein.

211. Section 537.525, RSMo. states as follows:

> 1. In addition to any other civil remedy available, the owner or lessee of the computer system, computer network, computer program, computer service, or data may bring a civil action against any person who violates sections 569.095 to 569.099, RSMo, for compensatory damages, including any expenditures reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, computer service, or data was not altered, damaged, or deleted by the access.
> 2. In any action brought pursuant to this section, the court may award reasonable attorney's fees to a prevailing plaintiff.

212. As used herein, Plaintiffs were the owner of computer programs and data to which BJC gained unauthorized access and made unauthorized use.

213. Section 569.095.1(3), RSMO. provides that a person "commits the offense of tampering with computer data if he or she knowingly and without authorization or without reasonable grounds to believe that he has such authorization: … (3) [d]iscloses or takes data … residing or existing internal or external to a computer, computer system or computer network."

214. BJC violated § 569.095.1(3) by knowingly and without authorization (or reasonable grounds to believe that it had authorization) disclosing or taking data residing internal or external

to a computer, computer system, or computer network – specifically Plaintiff's personal computing device and the data relating to his communications with BJC.

215. Section 569.095.1(5), RSMo. provides that a person "commits the offense of tampering with computer data if he or she knowingly and without authorization or without reasonable grounds to believe that he has such authorization: … (5) [a]ccesses a computer, a computer system, or a computer network, and intentionally examines information about another person."

216. BJC violated §569.095.1(5), RSMo. by knowingly and without authorization (or reasonable grounds to believe that it had authorization) accessing Plaintiff's personal computing device and examining information about Plaintiff.

217. Section 569.095.1(6), RSMo. provides that a person "commits the offense of tampering with computer data if he or she knowingly and without authorization or without reasonable grounds to believe that he has such authorization: …(6) [r]eceives, retains, uses, or discloses any data he knows or believes was obtained in violation of this subsection."

218. BJC violated §569.095.1(6), RSMo., by receiving, retaining, using, and disclosing data BJC knew or believed was obtained in violation of §569.095 – namely the personally identifiable patient data and re-directed communications that BJC used for marketing purposes without authorization.

219. Section 569.099(1), RSMo. provides that a person "commits the offense of tampering with computer users if he or she knowingly and without authorization or without reasonable grounds to believe that he has such authorization: (1) [a]ccesses or causes to be accessed any computer, computer system, or computer network[.]"

220. BJC violated §569.099.1(1), RSMo. in that it knowingly and without authorization (or reasonable grounds to believe that it had authorization) accessed Plaintiff's computing device for marketing purposes and thereby caused transmission of Plaintiff's personally identifiable data and re-directed communications to Facebook, Google, and theTradeDesk.

221. As a direct and proximate result of BJC's violations of § 569.099, Plaintiffs and patient Class Members were damaged by BJC in that:

a. BJC harmed Plaintiffs and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no more;

c. BJC eroded the essential confidential nature of the provider-patient relationship;

d. BJC took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs and Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included BJC's duty to maintain confidentiality; and

f. BJC's actions diminished the value of Plaintiffs and Class Members' personal information.

WHEREFORE, on behalf of himself and others, Plaintiffs pray judgment against Defendant for an amount excess of $25,000 that is fair, just, and reasonable and for the costs

expended herein, for post-judgment interest on said sums, and for such other relief as the Court deems just and proper.

COUNT V
IDENTITY THEFT – § 570.223, RSMo.

222. Plaintiffs incorporates all preceding paragraphs as if set forth fully herein.

223. Section 570.223, RSMo. provides that a person "commits the offense of identity theft if he or she knowingly and with the intent to deceive or defraud obtains, possesses, transfers, uses, or attempts to obtain, transfer, or use, one or more means of identification not lawfully issued for his or her use."

224. "Deceive" is defined as "making a representation which is false and which the actor does not believe to be true and upon which the victim relies, as to a matter of fact, law, value, intention or other state of mind, or concealing a material fact as to the terms of a contract or agreement." § 570.010(8), RSMo.

225. "Means of identification" is defined as "*anything* used by a person as a means to uniquely distinguish himself or herself." § 570.010(15), RSMo., emphasis added.

226. BJC committed identity theft under § 570.223 by knowingly obtaining and using Plaintiff's means of identification in the form of IP addresses, cookie identifiers, account numbers, and browser-fingerprint information for its own use without Plaintiffs' authorization.

227. BJC's use of Plaintiffs' means of identification occurred through the use of source code that caused Plaintiff's computing device to make fraudulent "postFORM" requests to Facebook that transmitted Plaintiffs' means of identification to Facebook for BJC's own purposes.

228. Section 570.223.4, RSMo. provides that "any person who commits an act made unlawful by subsection 1 of this section shall be liable to the person to whom the identifying information belonged for civil damages of up to five thousand dollars for each incident, or three

times the amount of actual damages, whichever amount is greater. A person damaged as set forth in subsection 1 of this section may also institute a civil action to enjoin and restrain future acts that would constitute a violation of subsection 1 of this section."

229. As a direct and proximate result of BJC's violation of § 570.223, Plaintiffs and patient Class Members were damaged by BJC in that:

a. BJC harmed Plaintiffs and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no more;

c. BJC eroded the essential confidential nature of the provider-patient relationship;

d. BJC took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiff and Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included BJC's duty to maintain confidentiality;

f. BJC's actions diminished the value of Plaintiffs and Class Members' personal information; and

g. Statutory damages as prescribed by § 570.223.4, RSMo.

WHEREFORE, on behalf of himself and others, Plaintiffs prays judgment against Defendant for an amount excess of $25,000 that is fair, just, and reasonable and for the costs

expended herein, for post-judgment interest on said sums, and for such other relief as the Court deems just and proper.

Respectfully Submitted,

THE SIMON LAW FIRM, P.C.

By: */s/ Amy Collignon Gunn*
Amy Collignon Gunn, #45016
Elizabeth S. Lenivy, #68469
800 Market Street, Suite 1700
St. Louis, Missouri 63101
P: (314) 241-2929
F: (314) 241-2020
agunn@simonlawpc.com
elenivy@simonlawpc.com
Attorneys for Plaintiffs

MISSOURI CIRCUIT COURT
TWENTY-SECOND JUDICIAL CIRCUIT
ST. LOUIS CITY

JOHN DOE I and JOHN DOE II, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	Cause No. 2222-CC09151
v.	)	Division 1
BJC HEALTH SYSTEM d/b/a BJC HEALTHCARE,	)	
Defendants.	)	

ENTRY OF APPEARANCE

COMES NOW Elizabeth S. Lenivy of The Simon Law Firm, P.C. and hereby enters her appearance on behalf of Plaintiffs John Doe I and John Doe II, and all others similarly situated.

Dated: July 28, 2022.

By: */s/ Elizabeth S. Lenivy*

Amy Collignon Gunn #45016
Elizabeth S. Lenivy #68469
Attorneys for Plaintiff
800 Market Street, Suite. 1700
St. Louis, MO 63101
Phone: (314) 241-2929
Fax: (314) 241-2029
agunn@simonlawpc.com
ewasham@simonlawpc.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies on July 28, 2022, the foregoing document was filed electronically with the St. Louis City Circuit Clerk using the Missouri Electronic Document Management System, which will send notice of electronic filing to the attorneys of record.

/s/ Elizabeth S. Lenivy

IN THE 22ND JUDICIAL CIRCUIT, CITY OF ST LOUIS, MISSOURI

Judge or Division: MICHAEL FRANCIS STELZER	**Case Number: 2222-CC09151**	
Plaintiff/Petitioner: JOHN DOE I vs.	Plaintiff's/Petitioner's Attorney/Address AMY KATHLEEN COLLIGNON GUNN 800 MARKET ST. SUITE 1700 SAINT LOUIS, MO 63101	
Defendant/Respondent: BJC HEALTH SYSTEM	Court Address: CIVIL COURTS BUILDING 10 N TUCKER BLVD SAINT LOUIS, MO 63101	(Date File Stamp)
Nature of Suit: CC Other Tort	Please see the attached information for appearing via WebEx. WebEx connection information may also be found at http://www.stlcitycircuitcourt.com/	

Summons in Civil Case

The State of Missouri to: BJC HEALTH SYSTEM
Alias: DBA BJC HEALTHCARE

CSC LAWYERS INC SERVICE CO
221 BOLIVAR STREET
JEFFERSON CITY, MO 65101

COLE COUNTY, MO

COURT SEAL OF
CITY OF ST LOUIS

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

*****Due to COVID19 challenges, virtual appearances by Webex.com are also required until further order of this Court. *****

If you have a disability requiring special assistance for your court appearance, please contact the court at least 48 hours in advance of scheduled hearing.

July 26, 2022 Thomas Kloeppinger

Date Clerk

Further Information:

Sheriff's or Server's Return

Note to serving officer: Summons should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

☐ delivering a copy of the summons and petition to the defendant/respondent.

☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.

☐ (for service on a corporation) delivering a copy of the summons and petition to: _____ (name) _____ (title).

☐ other: _____.

Served at _____ (address)

in _____ (County/City of St. Louis), MO, on _____ (date) at _____ (time).

_____ Printed Name of Sheriff or Server

_____ Signature of Sheriff or Server

Must be sworn before a notary public if not served by an authorized officer:

Subscribed and sworn to before me on _____ (date).

(Seal)

My commission expires: _____ Date

_____ Notary Public

Sheriff's Fees, if applicable

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	**$**_____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

MISSOURI CIRCUIT COURT
TWENTY-SECOND JUDICIAL CIRCUIT
ST. LOUIS CITY

JOHN DOE I and JOHN DOE II, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	Cause No. 2222-CC09151
v.	)	Division 1
BJC HEALTH SYSTEM d/b/a BJC HEALTHCARE,	)	
Defendants.	)	

ENTRY OF APPEARANCE

COMES NOW Jason Barnes of Simmons Hanly Conroy and hereby enters his appearance on behalf of Plaintiffs John Doe I and John Doe II, and all others similarly situated.

Dated: July 28, 2022.

/s/ Jason Barnes
Jason 'Jay' Barnes, 57583
Eric S. Johnson, 61680
An Truong (pro hac vice)
SIMMONS HANLY CONROY
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
jaybarnes@simmonsfirm.com
ejohnson@simmonsfirm.com
atruong@simmonsfirm.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies on July 28, 2022, the foregoing document was filed electronically with the St. Louis City Circuit Clerk using the Missouri Electronic Document Management System, which will send notice of electronic filing to the attorneys of record.

/s/ *Jason Barnes*

MISSOURI CIRCUIT COURT
TWENTY-SECOND JUDICIAL CIRCUIT
ST. LOUIS CITY

JOHN DOE I and JOHN DOE II, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	Cause No. 2222-CC09151
v.	)	Division 1
BJC HEALTH SYSTEM d/b/a BJC HEALTHCARE,	)	
Defendants.	)	

ENTRY OF APPEARANCE

COMES NOW Eric Johnson of Simmons Hanly Conroy and hereby enters his appearance on behalf of Plaintiffs John Doe I and John Doe II, and all others similarly situated.

Dated: July 28, 2022.

/s/ Eric Johnson
Jason 'Jay' Barnes, 57583
Eric Johnson, 61680
An Truong (pro hac vice)
SIMMONS HANLY CONROY
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
jaybarnes@simmonsfirm.com
ejohnson@simmonsfirm.com
atruong@simmonsfirm.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies on July 28, 2022, the foregoing document was filed electronically with the St. Louis City Circuit Clerk using the Missouri Electronic Document Management System, which will send notice of electronic filing to the attorneys of record.

*/s/ Eric Johnson /**

IN THE 22ND JUDICIAL CIRCUIT, CITY OF ST LOUIS, MISSOURI

FILED
22ND JUDICIAL CIRCUIT
CIRCUIT CLERK'S OFFICE
22 AUG -5 AM 1:50

Judge or Division: MICHAEL FRANCIS STELZER	**Case Number: 2222-CC09151**
Plaintiff/Petitioner: JOHN DOE I vs.	Plaintiff's/Petitioner's Attorney/Address AMY KATHLEEN COLLIGNON GUNN 800 MARKET ST. SUITE 1700 SAINT LOUIS, MO 63101
Defendant/Respondent: BJC HEALTH SYSTEM	Court Address: CIVIL COURTS BUILDING 10 N TUCKER BLVD SAINT LOUIS, MO 63101
Nature of Suit: CC Other Tort	Please see the attached information for appearing via WebEx. WebEx connection information may also be found at **http://www.stlcitycircuitcourt.com/**

RECEIVED
AUG 01 2022
COLE COUNTY
SHERIFF'S OFFICE
(Date File Stamp)

Summons in Civil Case

The State of Missouri to: BJC HEALTH SYSTEM
Alias: DBA BJC HEALTHCARE

CSC LAWYERS INC SERVICE CO
221 BOLIVAR STREET
JEFFERSON CITY, MO 65101

COLE COUNTY, MO

COURT SEAL OF
CITY OF ST LOUIS

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

*****Due to COVID19 challenges, virtual appearances by Webex.com are also required until further order of this Court. *****

If you have a disability requiring special assistance for your court appearance, please contact the court at least 48 hours in advance of scheduled hearing.

July 26, 2022 — Date

Thomas Klepfinger — Clerk

Further Information:

Sheriff's or Server's Return

ENTERED
AUG 05 2022
PAC

Note to serving officer: Summons should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

☐ delivering a copy of the summons and petition to the defendant/respondent.

☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.

☒ (for service on a corporation) delivering a copy of the summons and petition to: CSC Lawyers S.L. (name) Designee (title).

☐ other: _____.

Served at 350 E. High (address)

in Cole (County/City of St. Louis), MO, on 8.3.22 (date) at 8:00 AM (time).

Sheriff John R Wheeler by _____
Printed Name of Sheriff or Server — Signature of Sheriff or Server

Must be sworn before a notary public if not served by an authorized officer:

Subscribed and sworn to before me on _____ (date).

(Seal)

My commission expires: _____ (Date) _____ Notary Public

$30.00
$20.00

Sheriff's Fees, if applicable

Summons $_____

Non Est $_____

Sheriff's Deputy Salary Supplemental Surcharge $ 10.00

Mileage $_____ (_____ miles @ $._____ per mile)

Total $_____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.